Computer Science

Hummer Project: A Program for Network-based Intrusion Detection[1]

Ethan W. Dereszynski
Myles McNally*
Department of Computer Science and Mathematics
Alma College
614 W. Superior
Alma, MI 48801
(04ewdere@alma.edu, mcnally@alma.edu)

This presentation will outline the workings of the network-based intrusion detection project entitled Hummer and my specific role in its development. The Hummer program has been in development at the University of Idaho for the last four years. Hummer utilizes different modules to facilitate the communication between multiple systems on a network. Each module represents a different ability of Hummer that is necessary to detect intrusions against systems on the network. For example, the SocketPO module facilitates communication between other Hummer modules on the same system and even Hummers running on foreign machines. This module of Hummer is responsible for maintaining all messages sent between multiple instances of Hummers and their respective modules, dispatching each message to the correct module and system upon receipt. Other modules include the Believability module, responsible for insuring the integrity of each system's data, and the Agent module that can dispatch various probing threads dubbed "Agents" to Hummer systems. The final result of the project is a comprehensive system for network intrusion detection that is easily fits into an existing network security system (i.e. firewalls, honeypots, etc.), thereby utilizing available tools to further the level of protection.

A majority of my work involved the development of the aforementioned Believability module and the creation of Decision Modules (DMs). The Believability module maintains a list of all current known users (domains) on the system, and associates each one with a set of events that have involved that domain. Each of these events impacts the domain's integrity rating in either a positive or negative way. Hummer can then examine this integrity rating before accepting data or requests from the specified domain. The DMs take in data from Hummer's probing tools and determine if an anomaly is occurring. An example would be the Process DM that I coded. This Decision Module polled each system on the network for information regarding its process load. If that load is above a threshold value it may constitute an attack on that system, and the DM would respond accordingly.

[1] This work was supported by DARPA, award number F30602-02-1-0165, Principle Investigator Dr. Deborah Frincke, University of Idaho